

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 3 年    3 月 2 5 日  
Date of Application:

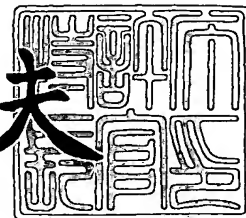
出 願 番 号            特 願 2 0 0 3 - 0 8 2 8 1 0  
Application Number:  
[ST. 10/C] :            [ J P 2 0 0 3 - 0 8 2 8 1 0 ]

出      願      人            パイオニア株式会社  
Applicant(s):

2 0 0 3 年 1 2 月 2 4 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号    出証特 2 0 0 3 - 3 1 0 6 7 5 9

【書類名】 特許願

【整理番号】 57P0033

【提出日】 平成15年 3月25日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 7/00  
H04L 9/00

【発明者】

【住所又は居所】 東京都大田区大森西4丁目15番5号 パイオニア株式会社  
大森工場内

【氏名】 浅井 亮介

【特許出願人】

【識別番号】 000005016

【氏名又は名称】 パイオニア株式会社

【代理人】

【識別番号】 100107331

【弁理士】

【氏名又は名称】 中村 聡延

【電話番号】 03-5524-2323

【選任した代理人】

【識別番号】 100104765

【弁理士】

【氏名又は名称】 江上 達夫

【電話番号】 03-5524-2323

【手数料の表示】

【予納台帳番号】 131957

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0104687

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ提供システム、方法およびプログラム

【特許請求の範囲】

【請求項 1】 サーバと端末装置とを備えるコンテンツ提供システムにおいて、

前記サーバは、

コンテンツの第 1 部分の要求に応じて、前記コンテンツの第 1 部分を前記端末装置へ送信する手段と、

前記コンテンツの第 2 部分の要求に応じて、前記コンテンツの第 2 部分を所定の方法で暗号化して前記端末装置へ送信する手段と、を備え、

前記端末装置は、

利用者の入力に応じて前記コンテンツの第 1 部分の要求を前記サーバへ送信する手段と、

前記コンテンツの第 1 部分を前記サーバから受信して保存する手段と、

前記コンテンツの第 2 部分の要求を前記サーバへ送信する手段と、

暗号化された前記コンテンツの第 2 部分を前記サーバから受信し、復号化して前記コンテンツの第 2 部分を取得する手段と、

前記コンテンツの第 1 部分及び第 2 部分を使用して当該コンテンツを復元する手段と、を備えることを特徴とするコンテンツ提供システム。

【請求項 2】 サーバと端末装置とを備えるコンテンツ提供システムにおいて、

前記サーバは、コンテンツの第 2 部分の要求に応じて、前記コンテンツの第 2 部分を所定の方法で暗号化して前記端末装置へ送信する手段を備え、

前記端末装置は、

前記コンテンツの第 1 部分を用意する手段と、

前記コンテンツの第 2 部分の要求を前記サーバへ送信する手段と、

暗号化された前記コンテンツの第 2 部分を前記サーバから受信し、復号化して前記コンテンツの第 2 部分を取得する手段と、

前記コンテンツの第 1 部分及び第 2 部分を使用して当該コンテンツを復元する

手段と、を備えることを特徴とするコンテンツ提供システム。

【請求項 3】 前記コンテンツの第 2 部分は、当該コンテンツを再生する時に継続的に必要な情報を含むことを特徴とする請求項 1 又は 2 に記載のコンテンツ提供システム。

【請求項 4】 前記コンテンツは動画コンテンツであり、前記コンテンツの第 2 部分は当該動画コンテンツを構成する動画データのヘッダ情報部分を含むことを特徴とする請求項 3 に記載のコンテンツ提供システム。

【請求項 5】 前記コンテンツは動画コンテンツであり、前記コンテンツの第 2 部分は当該動画コンテンツのストーリー中の特定の一部分に対応するデータを含むことを特徴とする請求項 3 に記載のコンテンツ提供システム。

【請求項 6】 前記コンテンツはプログラムであり、前記コンテンツの第 2 部分は当該プログラムにおいて使用される関数を規定するデータであることを特徴とする請求項 3 に記載のコンテンツ提供システム。

【請求項 7】 前記第 2 部分の要求は、当該コンテンツを再生するときに継続的に送信されることを特徴とする請求項 1 乃至 6 のいずれか一項に記載のコンテンツ提供システム。

【請求項 8】 前記第 2 部分の要求は、当該コンテンツの第 1 部分の少なくとも一部又は特定情報を含み、

前記サーバは、当該第 2 部分の要求を認証し、認証が正しく行われた場合に前記第 2 部分を前記端末装置に送信することを特徴とする請求項 1 乃至 7 のいずれか一項に記載のコンテンツ提供システム。

【請求項 9】 前記認証は、前記サーバが前記端末装置へ過去に送信したコンテンツの第 1 部分と、当該第 2 部分の要求に含まれる前記第 1 部分の少なくとも一部又は前記特定情報により特定されるコンテンツの第 1 部分との同一性に基づいて判断されることを特徴とする請求項 8 に記載のコンテンツ提供システム。

【請求項 10】 前記第 2 部分の要求に含まれる前記第 1 部分の少なくとも一部又は前記特定情報暗号化されていることを特徴とする請求項 9 に記載のコンテンツ提供システム。

【請求項 11】 前記暗号化に使用される鍵情報は、前記第 1 部分の少なく

とも一部又は前記特定情報の暗号化の時刻情報を含むことを特徴とする請求項 10 に記載のコンテンツ提供システム。

【請求項 12】 前記サーバは、複数の端末装置に対して同一の前記第 2 部分を送信することを特徴とする請求項 1 又は 2 に記載のコンテンツ提供システム。

【請求項 13】 前記サーバは、複数の端末装置の各々に対して異なる前記第 2 部分を送信することを特徴とする請求項 1 又は 2 に記載のコンテンツ提供システム。

【請求項 14】 前記第 2 部分は共通部分と個別部分により構成され、前記サーバは、複数の端末装置に対して、同一の共通部分と、それぞれ異なる個別部分の組み合わせを送信することを特徴とする請求項 1 又は 2 に記載のコンテンツ提供システム。

【請求項 15】 サーバと端末装置とを備えるシステムで実行されるコンテンツ提供方法において、

利用者の入力に応じてコンテンツの第 1 部分の要求を前記端末装置から前記サーバへ送信するステップと、

前記コンテンツの第 1 部分の要求に応じて、前記コンテンツの第 1 部分を前記サーバから前記端末装置へ送信するステップと、

前記端末装置において、前記コンテンツの第 1 部分を前記サーバから受信して保存するステップと、

前記端末装置において、前記コンテンツの第 2 部分の要求を前記サーバへ送信するステップと、

前記サーバにおいて、前記第 2 部分の要求に応じて、前記コンテンツの第 2 部分を所定の方法で暗号化して前記端末装置へ送信するステップと、

前記端末装置において、暗号化された前記コンテンツの第 2 部分を前記サーバから受信し、復号化して前記コンテンツの第 2 部分を取得するステップと、

前記端末装置において、前記コンテンツの第 1 部分及び第 2 部分を使用して当該コンテンツを復元するステップと、を有することを特徴とするコンテンツ提供方法。

【請求項 16】 サーバと端末装置とを備えるシステムで実行されるコンテンツ提供方法において、

前記端末装置において、前記コンテンツの第 1 部分を用意するステップと、

前記コンテンツの第 2 部分の要求を前記端末装置から前記サーバへ送信するステップと、

前記第 2 部分の要求に応じて、前記コンテンツの第 2 部分を所定の方法で暗号化して前記サーバから前記端末装置へ送信するステップと、

前記端末装置において、暗号化された前記コンテンツの第 2 部分を前記サーバから受信し、復号化して前記コンテンツの第 2 部分を取得するステップと、

前記コンテンツの第 1 部分及び第 2 部分を使用して当該コンテンツを復元するステップと、を有することを特徴とするコンテンツ提供方法。

【請求項 17】 サーバと端末装置を備えるコンテンツ提供システムのサーバであって、前記端末装置は、利用者の入力に応じてコンテンツの第 1 部分の要求を前記サーバへ送信する手段と、前記コンテンツの第 1 部分を前記サーバから受信して保存する手段と、前記コンテンツの第 2 部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第 2 部分を前記サーバから受信し、復号化して前記コンテンツの第 2 部分を取得する手段と、前記コンテンツの第 1 部分及び第 2 部分を使用して当該コンテンツを復元する手段と、を備え、

前記サーバは、コンテンツの第 1 部分の要求に応じて、前記コンテンツの第 1 部分を前記端末装置へ送信する手段と、前記コンテンツの第 2 部分の要求に応じて、前記コンテンツの第 2 部分を所定の方法で暗号化して前記端末装置へ送信する手段と、を備えることを特徴とするサーバ。

【請求項 18】 サーバと端末装置を備えるコンテンツ提供システムの端末装置であって、前記サーバは、コンテンツの第 1 部分の要求に応じて、前記コンテンツの第 1 部分を前記端末装置へ送信する手段と、前記コンテンツの第 2 部分の要求に応じて、前記コンテンツの第 2 部分を所定の方法で暗号化して前記端末装置へ送信する手段と、を備え、

前記端末装置は、利用者の入力に応じてコンテンツの第 1 部分の要求を前記サーバへ送信する手段と、前記コンテンツの第 1 部分を前記サーバから受信して保

存する手段と、前記コンテンツの第 2 部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第 2 部分を前記サーバから受信し、復号化して前記コンテンツの第 2 部分を取得する手段と、前記コンテンツの第 1 部分及び第 2 部分を使用して当該コンテンツを復元する手段と、を備えることを特徴とする端末装置。

【請求項 19】 サーバと端末装置を備えるコンテンツ提供システムのサーバにおいて、前記端末装置は、前記コンテンツの第 1 部分を用意する手段と、前記コンテンツの第 2 部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第 2 部分を前記サーバから受信し、復号化して前記コンテンツの第 2 部分を取得する手段と、前記コンテンツの第 1 部分及び第 2 部分を使用して当該コンテンツを復元する手段と、を備え、

前記サーバは、コンテンツの第 2 部分の要求に応じて、前記コンテンツの第 2 部分を所定の方法で暗号化して前記端末装置へ送信する手段を備えることを特徴とするサーバ。

【請求項 20】 サーバと端末装置を備えるコンテンツ提供システムの端末装置において、前記サーバは、コンテンツの第 2 部分の要求に応じて、前記コンテンツの第 2 部分を所定の方法で暗号化して前記端末装置へ送信する手段を備え、

前記端末装置は、前記コンテンツの第 1 部分を用意する手段と、前記コンテンツの第 2 部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第 2 部分を前記サーバから受信し、復号化して前記コンテンツの第 2 部分を取得する手段と、前記コンテンツの第 1 部分及び第 2 部分を使用して当該コンテンツを復元する手段と、を備えることを特徴とする端末装置。

【請求項 21】 サーバと端末装置を備えるコンテンツ提供システムのサーバにおいて実行されるコンテンツ提供プログラムであって、前記端末装置は、利用者の入力に応じてコンテンツの第 1 部分の要求を前記サーバへ送信する手段と、前記コンテンツの第 1 部分を前記サーバから受信して保存する手段と、前記コンテンツの第 2 部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第 2 部分を前記サーバから受信し、復号化して前記コンテンツの第 2

部分を取得する手段と、前記コンテンツの第1部分及び第2部分を使用して当該コンテンツを復元する手段と、を備え、

前記サーバを、コンテンツの第1部分の要求に応じて、前記コンテンツの第1部分を前記端末装置へ送信する手段、および、前記コンテンツの第2部分の要求に応じて、前記コンテンツの第2部分を所定の方法で暗号化して前記端末装置へ送信する手段、として機能させることを特徴とするコンテンツ提供プログラム。

【請求項22】 サーバと端末装置を備えるコンテンツ提供システムの端末装置において実行されるコンテンツ提供プログラムであって、前記サーバは、コンテンツの第1部分の要求に応じて、前記コンテンツの第1部分を前記端末装置へ送信する手段と、前記コンテンツの第2部分の要求に応じて、前記コンテンツの第2部分を所定の方法で暗号化して前記端末装置へ送信する手段と、を備え、

前記端末装置を、利用者の入力に応じてコンテンツの第1部分の要求を前記サーバへ送信する手段、前記コンテンツの第1部分を前記サーバから受信して保存する手段、前記コンテンツの第2部分の要求を前記サーバへ送信する手段、暗号化された前記コンテンツの第2部分を前記サーバから受信し、復号化して前記コンテンツの第2部分を取得する手段、および、前記コンテンツの第1部分及び第2部分を使用して当該コンテンツを復元する手段、として機能させることを特徴とするコンテンツ提供プログラム。

【請求項23】 サーバと端末装置を備えるコンテンツ提供システムのサーバにおいて実行されるコンテンツ提供プログラムにおいて、前記端末装置は、前記コンテンツの第1部分を用意する手段と、前記コンテンツの第2部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第2部分を前記サーバから受信し、復号化して前記コンテンツの第2部分を取得する手段と、前記コンテンツの第1部分及び第2部分を使用して当該コンテンツを復元する手段と、を備え、

前記サーバを、コンテンツの第2部分の要求に応じて、前記コンテンツの第2部分を所定の方法で暗号化して前記端末装置へ送信する手段として機能させることを特徴とするコンテンツ提供プログラム。

【請求項24】 サーバと端末装置を備えるコンテンツ提供システムの端末

装置において実行されるコンテンツ提供プログラムにおいて、前記サーバは、コンテンツの第2部分の要求に応じて、前記コンテンツの第2部分を所定の方法で暗号化して前記端末装置へ送信する手段を備え、

前記端末装置を、前記コンテンツの第1部分を用意する手段、前記コンテンツの第2部分の要求を前記サーバへ送信する手段、暗号化された前記コンテンツの第2部分を前記サーバから受信し、復号化して前記コンテンツの第2部分を取得する手段、および、前記コンテンツの第1部分及び第2部分を使用して当該コンテンツを復元する手段、として機能させることを特徴とするコンテンツ提供プログラム。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

本発明は、映像情報、音声情報などを含む各種情報を提供する手法に関する。

##### 【0002】

#### 【従来の技術】

通信路や放送などを利用してサーバやセンター装置など（以下、まとめて「サーバ」と呼ぶ。）から利用者が映像情報、音声情報、その他の各種情報（以下、「コンテンツ」と呼ぶ。）を取得することが行われている。コンテンツの代表的なものとしては、映画などの映像及び音声情報、音楽などの音声情報、コンピュータのプログラムやデータなどがあり、これらをサーバ装置からネットワークその他の通信路（パス）を介して利用者の端末装置（クライアント）へ送信することが行われている。なお、そのような経路の代表的なものとしてはインターネットが挙げられる。

##### 【0003】

この場合、クライアントに情報記憶領域を備え、サーバから提供されたコンテンツを情報記憶領域内に記憶することにより、その情報の利用上の利便性を高めることが行われている。例えば映像及び音声情報などの場合、サーバから提供されたコンテンツを一旦クライアントの情報記憶領域に記憶すれば、利用者は好きな時間にそのコンテンツを再生して楽しむことができる。

**【0004】**

しかし、コンテンツが一旦クライアントの情報記憶領域に保存されると、そのコンテンツの複製などの悪用が可能となる。クライアントの情報記憶領域内に保存されたコンテンツを不正に再生したり、複製したりすることは比較的容易であるが、コンテンツが著作物である場合、有料コンテンツである場合などにはこれが問題となる。クライアントの情報記憶領域内に保存されたコンテンツの複製を防ぐため、コンテンツを暗号化して提供するなどの各種の対策が行われているが、暗号が不正に解読される可能性は排除できない。また、暗号の解読を困難にするためにコンテンツに対して複雑な暗号化処理を施すと、暗号の解読は困難になるものの、正当な利用者がコンテンツを再生する際の復号化に時間を要し、円滑な再生に支障を生じるなどの問題もある。

**【0005】**

このような観点から、コンテンツ全体を一度に提供するのではなく、一部を分割して提供する方法が提案されている。例えば、デジタル放送に関連して、不完全な番組データを放送する一方、複製管理情報を通信回線を介して送信し、両者によって完全な番組データを復元する手法が提案されている（特許文献1参照）。また、コンテンツを部分的に劣化させた不完全ファイルを先に送信した後、これを補完する核ファイルを別個に送信し、受信した利用者側で不完全ファイルと核ファイルにより完全映像を復元する方法も提案されている（特許文献2参照）。さらに、コンテンツの一部を欠損させた状態で送信し、その後に欠損部分を提供する際に課金を行うシステムも提案されている（特許文献3参照）。

**【0006】****【特許文献1】**

特開 2002-9716 号公報

**【特許文献2】**

特開平 10-336625 号公報

**【特許文献3】**

特開 2002-16899 号公報

**【0007】**

**【発明が解決しようとする課題】**

上記のようにコンテンツの一部を分割して別個に提供する方法では、分割した各部分の作り方やそれらの提供方法などにより、その有効性が大きく影響される。本発明は、コンテンツの一部を分割して提供する方法において、分割や提供方法を工夫することにより、コンテンツの不正な複製や使用などを効果的に防止することを課題とする。

**【0008】****【課題を解決するための手段】**

請求項1に記載の発明は、サーバと端末装置とを備えるコンテンツ提供システムにおいて、前記サーバは、コンテンツの第1部分の要求に応じて、前記コンテンツの第1部分を前記端末装置へ送信する手段と、前記コンテンツの第2部分の要求に応じて、前記コンテンツの第2部分を所定の方法で暗号化して前記端末装置へ送信する手段と、を備え、前記端末装置は、利用者の入力に応じて前記コンテンツの第1部分の要求を前記サーバへ送信する手段と、前記コンテンツの第1部分を前記サーバから受信して保存する手段と、前記コンテンツの第2部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第2部分を前記サーバから受信し、復号化して前記コンテンツの第2部分を取得する手段と、前記コンテンツの第1部分及び第2部分を使用して当該コンテンツを復元する手段と、を備えることを特徴とする。

**【0009】**

請求項2に記載の発明は、サーバと端末装置とを備えるコンテンツ提供システムにおいて、前記サーバは、コンテンツの第2部分の要求に応じて、前記コンテンツの第2部分を所定の方法で暗号化して前記端末装置へ送信する手段を備え、前記端末装置は、前記コンテンツの第1部分を用意する手段と、前記コンテンツの第2部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第2部分を前記サーバから受信し、復号化して前記コンテンツの第2部分を取得する手段と、前記コンテンツの第1部分及び第2部分を使用して当該コンテンツを復元する手段と、を備えることを特徴とする。

**【0010】**

請求項 15 に記載の発明は、サーバと端末装置とを備えるシステムで実行されるコンテンツ提供方法において、利用者の入力に応じてコンテンツの第 1 部分の要求を前記端末装置から前記サーバへ送信するステップと、前記コンテンツの第 1 部分の要求に応じて、前記コンテンツの第 1 部分を前記サーバから前記端末装置へ送信するステップと、前記端末装置において、前記コンテンツの第 1 部分を前記サーバから受信して保存するステップと、前記端末装置において、前記コンテンツの第 2 部分の要求を前記サーバへ送信するステップと、前記サーバにおいて、前記第 2 部分の要求に応じて、前記コンテンツの第 2 部分を所定の方法で暗号化して前記端末装置へ送信するステップと、前記端末装置において、暗号化された前記コンテンツの第 2 部分を前記サーバから受信し、復号化して前記コンテンツの第 2 部分を取得するステップと、前記端末装置において、前記コンテンツの第 1 部分及び第 2 部分を使用して当該コンテンツを復元するステップと、を有することを特徴とする。

#### 【0011】

請求項 16 に記載の発明は、サーバと端末装置とを備えるシステムで実行されるコンテンツ提供方法において、前記端末装置において、前記コンテンツの第 1 部分を用意するステップと、前記コンテンツの第 2 部分の要求を前記端末装置から前記サーバへ送信するステップと、前記第 2 部分の要求に応じて、前記コンテンツの第 2 部分を所定の方法で暗号化して前記サーバから前記端末装置へ送信するステップと、前記端末装置において、暗号化された前記コンテンツの第 2 部分を前記サーバから受信し、復号化して前記コンテンツの第 2 部分を取得するステップと、前記コンテンツの第 1 部分及び第 2 部分を使用して当該コンテンツを復元するステップと、を有することを特徴とする。

#### 【0012】

請求項 17 に記載の発明は、サーバと端末装置を備えるコンテンツ提供システムのサーバであって、前記端末装置は、利用者の入力に応じてコンテンツの第 1 部分の要求を前記サーバへ送信する手段と、前記コンテンツの第 1 部分を前記サーバから受信して保存する手段と、前記コンテンツの第 2 部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第 2 部分を前記サーバから

受信し、復号化して前記コンテンツの第 2 部分を取得する手段と、前記コンテンツの第 1 部分及び第 2 部分を使用して当該コンテンツを復元する手段と、を備え、前記サーバは、コンテンツの第 1 部分の要求に応じて、前記コンテンツの第 1 部分を前記端末装置へ送信する手段と、前記コンテンツの第 2 部分の要求に応じて、前記コンテンツの第 2 部分を所定の方法で暗号化して前記端末装置へ送信する手段と、を備えることを特徴とする。

#### 【0013】

請求項 18 に記載の発明は、サーバと端末装置を備えるコンテンツ提供システムの端末装置であって、前記サーバは、コンテンツの第 1 部分の要求に応じて、前記コンテンツの第 1 部分を前記端末装置へ送信する手段と、前記コンテンツの第 2 部分の要求に応じて、前記コンテンツの第 2 部分を所定の方法で暗号化して前記端末装置へ送信する手段と、を備え、前記端末装置は、利用者の入力に応じてコンテンツの第 1 部分の要求を前記サーバへ送信する手段と、前記コンテンツの第 1 部分を前記サーバから受信して保存する手段と、前記コンテンツの第 2 部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第 2 部分を前記サーバから受信し、復号化して前記コンテンツの第 2 部分を取得する手段と、前記コンテンツの第 1 部分及び第 2 部分を使用して当該コンテンツを復元する手段と、を備えることを特徴とする。

#### 【0014】

請求項 19 に記載の発明は、サーバと端末装置を備えるコンテンツ提供システムのサーバにおいて、前記端末装置は、前記コンテンツの第 1 部分を用意する手段と、前記コンテンツの第 2 部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第 2 部分を前記サーバから受信し、復号化して前記コンテンツの第 2 部分を取得する手段と、前記コンテンツの第 1 部分及び第 2 部分を使用して当該コンテンツを復元する手段と、を備え、前記サーバは、コンテンツの第 2 部分の要求に応じて、前記コンテンツの第 2 部分を所定の方法で暗号化して前記端末装置へ送信する手段を備えることを特徴とする。

#### 【0015】

請求項 20 に記載の発明は、サーバと端末装置を備えるコンテンツ提供システ

ムの端末装置において、前記サーバは、コンテンツの第2部分の要求に応じて、前記コンテンツの第2部分を所定の方法で暗号化して前記端末装置へ送信する手段を備え、前記端末装置は、前記コンテンツの第1部分を用意する手段と、前記コンテンツの第2部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第2部分を前記サーバから受信し、復号化して前記コンテンツの第2部分を取得する手段と、前記コンテンツの第1部分及び第2部分を使用して当該コンテンツを復元する手段と、を備えることを特徴とする。

#### 【0016】

請求項21に記載の発明は、サーバと端末装置を備えるコンテンツ提供システムのサーバにおいて実行されるコンテンツ提供プログラムであって、前記端末装置は、利用者の入力に応じてコンテンツの第1部分の要求を前記サーバへ送信する手段と、前記コンテンツの第1部分を前記サーバから受信して保存する手段と、前記コンテンツの第2部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第2部分を前記サーバから受信し、復号化して前記コンテンツの第2部分を取得する手段と、前記コンテンツの第1部分及び第2部分を使用して当該コンテンツを復元する手段と、を備え、前記サーバを、コンテンツの第1部分の要求に応じて、前記コンテンツの第1部分を前記端末装置へ送信する手段、および、前記コンテンツの第2部分の要求に応じて、前記コンテンツの第2部分を所定の方法で暗号化して前記端末装置へ送信する手段、として機能させることを特徴とする。

#### 【0017】

請求項22に記載の発明は、サーバと端末装置を備えるコンテンツ提供システムの端末装置において実行されるコンテンツ提供プログラムであって、前記サーバは、コンテンツの第1部分の要求に応じて、前記コンテンツの第1部分を前記端末装置へ送信する手段と、前記コンテンツの第2部分の要求に応じて、前記コンテンツの第2部分を所定の方法で暗号化して前記端末装置へ送信する手段と、を備え、前記端末装置を、利用者の入力に応じてコンテンツの第1部分の要求を前記サーバへ送信する手段、前記コンテンツの第1部分を前記サーバから受信して保存する手段、前記コンテンツの第2部分の要求を前記サーバへ送信する手段

、暗号化された前記コンテンツの第2部分を前記サーバから受信し、復号化して前記コンテンツの第2部分を取得する手段、および、前記コンテンツの第1部分及び第2部分を使用して当該コンテンツを復元する手段、として機能させることを特徴とする。

#### 【0018】

請求項23に記載の発明は、サーバと端末装置を備えるコンテンツ提供システムのサーバにおいて実行されるコンテンツ提供プログラムにおいて、前記端末装置は、前記コンテンツの第1部分を用意する手段と、前記コンテンツの第2部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第2部分を前記サーバから受信し、復号化して前記コンテンツの第2部分を取得する手段と、前記コンテンツの第1部分及び第2部分を使用して当該コンテンツを復元する手段と、を備え、前記サーバを、コンテンツの第2部分の要求に応じて、前記コンテンツの第2部分を所定の方法で暗号化して前記端末装置へ送信する手段として機能させることを特徴とする。

#### 【0019】

請求項24に記載の発明は、サーバと端末装置を備えるコンテンツ提供システムの端末装置において実行されるコンテンツ提供プログラムにおいて、前記サーバは、コンテンツの第2部分の要求に応じて、前記コンテンツの第2部分を所定の方法で暗号化して前記端末装置へ送信する手段を備え、前記端末装置を、前記コンテンツの第1部分を用意する手段、前記コンテンツの第2部分の要求を前記サーバへ送信する手段、暗号化された前記コンテンツの第2部分を前記サーバから受信し、復号化して前記コンテンツの第2部分を取得する手段、および、前記コンテンツの第1部分及び第2部分を使用して当該コンテンツを復元する手段、として機能させることを特徴とする。

#### 【0020】

##### 【発明の実施の形態】

以下、本発明の好適な実施形態について説明する。本発明は、通信路や放送などを利用して利用者にコンテンツを提供するシステムに関する。本実施形態では、コンテンツを保有するサーバから利用者の端末装置（クライアント）へコンテ

ンツを提供する例について説明する。なお、本発明における「コンテンツ」には、映画などの映像・音声情報、静止画などの画像情報、音楽などの音声情報、各種プログラム、その他の各種データを含むものとする。

#### 【0021】

本実施形態では、利用者へ提供すべきコンテンツをコア部分と非コア部分とに分け、コア部分に必要な暗号化処理などを施してクライアントへ提供することを基本的な特徴とする。図1 (a) にコンテンツの概略構成を模式的に示す。図1 (a) に示すように、コンテンツ10は、コア部分12と、コア部分以外の部分11 (以下、「非コア部分」と呼ぶ。) とに分けられる。即ち、コア部分12と非コア部分11とを併せて、例えば映画1本などの1つのコンテンツ10が構成される。なお、非コア部分11をコンテンツ10の大半を占める部分とし、コア部分12をある程度小さなサイズとすることが望ましい。ここで、本発明では、コア部分12は、コンテンツ10において重要な部分や、利用者によるコンテンツ10の再生や利用において継続的に必要な部分などとする。

#### 【0022】

図1 (b) に本実施形態による、基本的なコンテンツ提供方法を模式的に示す。図示のように、コンテンツを提供するシステムでは、サーバ1とクライアント2が通信路などにより情報伝送可能に構成されている。

#### 【0023】

サーバ1は、クライアント2からの要求に応じて、指定されたコンテンツ10をクライアント2へ送信する。コンテンツ10は図1 (a) に示すようにコア部分12と非コア部分11とにより構成されている。クライアント2からあるコンテンツ10の要求を受け取ると、サーバ1は非コア部分11を基本的にそのままクライアント2へ送信するとともに、コア部分12を所定の暗号化処理を施した上でクライアント2に送信する。

#### 【0024】

サーバ1は、提供すべきコンテンツのコア部分を保有する、認証機能を持った安全なサーバとする。そして、サーバ1は、コア部分12がいかなる場合もクライアント2の無防備な記憶領域に書き込まれないようにする。

## 【0025】

非コア部分 11 は、コンテンツ 10 の大半を占める部分であるが、暗号化処理などが施されていない。一方、コア部分 12 は非コア部分 11 と比較してデータ量の小さい部分であるが、コンテンツ 10 の再生や使用に不可欠な部分であるため、クライアント 2 は暗号化されたコア部分 12 を取得し、正しく復号化しないとコンテンツ 10 全体を実質的に再生、使用することができない。よって、自身に蓄積されているように見えるコンテンツをクライアント 2 が使用する際には、クライアント 2 は必ずサーバ 1 から不足しているコア情報 12 を取得する必要がある。

## 【0026】

この方法によれば、コンテンツの重要部分をコア部分とし、これを暗号化して送信するので、コア部分のみの暗号化処理によりコンテンツ全体を実質的に保護することが可能となる。この場合、暗号化処理の対象はコンテンツの一部であるコア部分のみとすることができるので、コンテンツ全体を暗号化する場合と比較してサーバ側の暗号化処理負荷を小さくすることができ、コンテンツの再生や利用時におけるクライアント側での復号化処理負荷も小さくすることができる。また、万が一クライアントが何らかの方法で解析された場合でも、そこにはコア部分は記憶されていないので、クライアントからコンテンツを価値ある形で取り出すことは不可能となる。

## 【0027】

具体的には、本発明の 1 つの好適な実施形態によれば、サーバと端末装置とを備えるコンテンツ提供システムにおいて、サーバは、コンテンツの第 2 部分の要求に応じて、前記コンテンツの第 2 部分を所定の方法で暗号化して前記端末装置へ送信する手段を備える。また、端末装置は、前記コンテンツの第 1 部分を用意する手段と、前記コンテンツの第 2 部分の要求を前記サーバへ送信する手段と、暗号化された前記コンテンツの第 2 部分を前記サーバから受信し、復号化して前記コンテンツの第 2 部分を取得する手段と、前記コンテンツの第 1 部分及び第 2 部分を使用して当該コンテンツを復元する手段と、を備える。

## 【0028】

上記のコンテンツ提供システムによれば、ユーザに対して提供されるべきコンテンツは、第1部分と第2部分により構成される。ユーザは、端末装置を利用し、必要に応じてサーバに接続してコンテンツを取得し、その再生や利用を行う。端末装置は、コンテンツの第1部分を各種の方法で用意することができる。例えば、端末装置はユーザが指定したコンテンツの第1部分をサーバへ要求し、それをサーバから受信することにより用意することができる。また、端末装置からの要求がなくても、サーバが定期的又は不定期に、特定の端末装置又は不特定多数の端末装置に対してコンテンツの第1部分を送信する処理を行っている場合には、端末装置はそれを受信することによりコンテンツの第1部分を用意することができる。これには、例えば放送サービスなどにより特定のコンテンツを配信する場合が該当する。また、コンテンツの第1部分は、サーバから受信する方法の他に、記憶媒体や記憶装置などから取得することも可能である。例えば、端末装置が過去にサーバなどから受信したコンテンツの第1部分を記憶する記憶部などを備える場合には、必要なときにその記憶部からコンテンツの第1部分を読み出すなどして用意することができる。さらに、コンテンツの第1部分が、通信によってではなく、例えばCD-ROMやDVD-ROMなどの各種の記憶媒体に記録された状態で配布、頒布されている場合には、端末装置はそのような記憶媒体から読み出すことにより、コンテンツの第1部分を用意することもできる。

#### 【0029】

##### 【実施例】

次に、図面を参照して本発明の好適な実施例を説明する。

#### 【0030】

##### [システム構成]

##### (基本構成)

図2に、本発明の実施例によるコンテンツ提供システムの概略構成を示す。図示のように、コンテンツ提供システムは、サーバ20とクライアント30とが通信路40を介して通信可能に接続されてなる。通信路40は、例えばインターネットなどのネットワークとすることができる。サーバ20は利用者に提供すべきコンテンツを保有し、必要に応じてクライアント30へ送信する役割を有する。

一方、クライアント 30 は利用者が使用する端末装置である。

#### 【0031】

図示のように、サーバ 20 は、コンテンツデータ記憶部 21 と、管理情報記憶部 22 と、コントロール部 23 と、通信部 24 とを備えて構成される。コンテンツデータ記憶部 21 は、利用者へ提供すべきコンテンツのデータを記憶するデータベースであり、例えばコンテンツとしての映画、音楽、所定のプログラム、その他のデータを記憶する。

#### 【0032】

管理情報記憶部 22 は、サーバ 20 からクライアント 30 へのコンテンツの提供における管理情報を記憶するデータベースである。管理情報としては、例えばどの利用者（クライアント）へどのコンテンツをいつ送ったか、その際のコア部分と非コア部分のデータはどのように決定されているかなど、コンテンツの提供に関する各種の情報を含む。通信部 24 はコンテンツ及びその他の情報を、通信路 40 を介してクライアント 30 へ送信する機能を有する。

#### 【0033】

コントロール部 23 は、サーバ 20 からクライアント 30 へのコンテンツ提供処理全体にわたる必要な制御を行う。具体的には、クライアント 30 から要求されたコンテンツをコンテンツデータ記憶部 21 から取り出したり、取り出したコンテンツに対して非コア部分とコア部分を設定したり、クライアント 30 へ送信したコンテンツの送信履歴情報（ログ情報）を記録したりといった各種の処理を行う。

#### 【0034】

一方、クライアント 30 は、通信部 31 と、コントロール部 32 と、一時記憶部 33 と、必要に応じて提示部 34 とを備える。通信部 31 は、サーバ 20 との情報の通信を行う部分である。一時記憶部 33 は、サーバ 20 から提供されたコンテンツ、具体的には非コア部分 11 を一時的に記憶する記憶部である。提示部 34 はクライアントの動作状況を提示したり、コンテンツを利用者へ提示する手段であり、映像を表示する表示装置、音声を出力するスピーカなどを含むことができる。また、クライアント 30 の種類などに応じて、提示部 34 はクライアン

ト 30 の内部に設けられている場合もあるし、クライアント 30 とは独立に設けられる場合もある。

#### 【0035】

コントロール部 32 は、必要な指示、指定などを通信部 31 及び通信路 40 を介してサーバ 20 へ送信したり、サーバ 20 から受信したコンテンツを一時記憶部 33 に記憶したり、提示部 34 へ供給して再生したりといった処理を行う。また、コンテンツの一部がコア部分として暗号化されて送信された場合は、それを復号化する認証処理も行う。

#### 【0036】

本実施例では、クライアントが要求したコンテンツは、図 1 (a) に示すようにコア部分 12 と非コア部分 11 とに分割され、コア部分 12 に対しては暗号化を施した上でクライアント 30 へ提供される。クライアント 30 は、非コア部分 11 を受信するとそのまま一時記憶部 33 へ記憶することができる。一方、クライアント 30 は、暗号化されたコア部分 12 をクライアント 30 内部には保存しない。即ち、コア部分 12 は、必要なときにクライアント 30 からサーバ 20 へ要求がなされ、その都度サーバ 20 からクライアント 30 へ送信される。クライアント 30 は、コア部分 12 を受信する度に、暗号化されたコア部分の復号および必要に応じて認証を行う。

#### 【0037】

コア部分 12 の暗号化に使用する鍵情報が暗号化の時刻情報を含むようにすることができる。具体的には、サーバ 20 がコア部分 12 をクライアント 30 へ送信する際にリアルタイムでコア部分 12 の暗号化を行う場合は、暗号化の時刻情報はサーバ 30 がそのコア部分 12 を暗号化するときの時刻情報を鍵情報とすることができる。また、クライアント 30 からコア部分 12 の要求を受け取ったときに、要求されたコア部分 12 をサーバ 30 が暗号化する場合には、クライアント 30 からのコア部分 12 の要求時の時刻情報を鍵情報とすることができる。

#### 【0038】

サーバ 20 から送信されたコア部分 12 がクライアント 30 内の一時記憶部 33 に記憶されないようにするにはいくつかの方法が存在する。例えば、コア部分

12については、そのデータ中に「そのデータをクライアントの一時記憶部33に記憶しないこと」を示すフラグなどを含めておく。クライアント32のコントロール部32はそのフラグを見て、受信したコア部分12を一時記憶部33に記憶しないこととする。

#### 【0039】

また、他の方法では、サーバ20が、クライアントのIDとコア部分12のデータをクライアントへ送信した時刻などの情報を組み合わせて認証情報を生成し、その認証情報が正しい場合にコア部分を取得可能とする。この場合は、コア部分12の情報はクライアント30の一時記憶部33に保存できることになるが、コア部分12の暗号化を解除するための認証情報は常に更新されているので、過去に一時記憶部33内に記憶しておいた認証情報ではコア部分の復号化が不能となる。

#### 【0040】

##### (変形例)

次に、本実施例のコンテンツ提供システムの変形例を説明する。図2に破線で示すように、サーバ20に加えてバッファサーバ50を設ける構成とすることもできる。この場合、サーバ20は各コンテンツ10のコア部分12のみを保存し、各クライアント30へ送信する。一方、バッファサーバ50は各コンテンツ10の非コア部分11のみを保存し、各クライアント30へ送信する。バッファサーバ50は、コンテンツ10の非コア部分11のデータを記憶するデータ記憶部52と、通信路40を介してクライアント30と通信するための通信部51とを備える。なお、バッファサーバ50は、クライアント30の数やコンテンツの数に応じて複数設けることができる。これにより、多数のクライアント30に対してコンテンツを提供する場合のサーバ20の負荷を軽減することが可能となる。

#### 【0041】

また、他の変形例を図3に示す。図3に示す変形例では、サーバ20とクライアント30との間に複数の通信路（パス）40及び41を設ける。通信路40は非コア部分専用の通信路とし、通信路41はコア部分専用の通信路としている。サーバ20内には、2つの通信路40及び41に対応して別個の通信部24及び

25が設けられ、クライアント30内にも2つの通信路40及び41に対応して別個の通信部35及び31が設けられる。このように、コア部分と非コア部分の通信路を別個にすることにより、コンテンツを通信路上から傍受しようとする不正者などが1つの通信路からコア部分と非コア部分の両方を取得することが不可能となる。なお、通信路を複数にする例としては、異なるネットワークを使用する方法、ネットワークと電話回線を使用する方法などが挙げられる。また、そのように通信路を物理的に別個とする他に、同一の通信路を異なる時間に使用することにより時間的に分割することや周波数的に分割すること、変調方式を変えて空間的に分割することも可能である。

#### 【0042】

##### [システムの動作]

次に、上述のコンテンツ提供システムの動作例について説明する。図4は本システムにより、サーバ20からクライアント30へコンテンツを提供する際の処理を示す図である。本例では、サーバ20からある映画などのコンテンツをクライアント30へ提供することとする。図4(a)はそのコンテンツを利用者が初めて視聴する場合の処理例であり、図4(b)は同一のコンテンツを利用者が繰り返し視聴する場合の2回目以降の視聴の処理例である。なお、図4の例では、1つのコンテンツが3つの非コア部分A～C及び1つのコア部分から構成されているものとする。

#### 【0043】

まず、初回の視聴においては、図4(a)に示すように、利用者がコンテンツ提供などのサービスを希望するとき、クライアント30を操作してコンテンツの送信を求める一次要求をサーバ20へ送信する。サーバ20は、一次要求に対して、コンテンツを構成する3つの非コア部分A～Cを順にクライアント30へ送信する。クライアント30は、非コア部分A～Cを順に受信し、クライアント30内の記憶部(例えば図2に示す一時記憶部33)に保存する。

#### 【0044】

非コア部分A～Cの受信が完了すると、クライアント30は不足しているコア部分を要求する補完要求をサーバ20へ送信する。サーバ20は補完要求を受信

し、コア部分をクライアント 30 へ送信する。クライアント 30 はコア部分を受信し、必要な復号化処理を行ってコア部分を復号化し、非コア部分 A～C 及びコア部分により構成されるコンテンツを復元して、再生、使用などする。なお、前述のように、クライアント 30 はコア部分を一時記憶部 33 内に記憶することはできない。

#### 【0045】

次に、2 回目以降の視聴について図 4 (b) を参照して説明する。2 回目以降の視聴では、利用者がコンテンツの視聴などのサービスを希望すると、クライアント 30 にその旨の指示などを入力する。これにより、クライアント 30 は初回の視聴において記憶した非コア部分 A～C を一時記憶部 33 から読み出す。しかし、コア部分はクライアント内の一時記憶部 33 には記憶されていないので、クライアント 30 はコア部分を要求する補完要求をサーバ 20 へ適宜送信する。

#### 【0046】

サーバ 20 は補完要求を受け取ると、コア部分に所定の暗号化などを施してクライアント 30 へ送信する。クライアント 30 は、受信したコア部分を復号化し、非コア部分 A～C 及びコア部分によりコンテンツを復元し、再生する。なお、2 回目以降の視聴においても、クライアント 30 はサーバ 20 から受信したコア部分をクライアント内部の一時記憶部 33 に記憶することはできない。

#### 【0047】

このように、提供すべきコンテンツのうち、非コア部分をクライアント内の記憶部に記憶可能とすることにより、2 回目以降にそのコンテンツを再生、視聴などする際に、非コア部分を再度送信する必要はなくなる。前述のように、非コア部分はコンテンツの大半を占める部分であるので、これによりコンテンツを無駄に繰り返し送信する必要がなくなる。一方、コア部分はクライアント内の記憶部に記憶できないので、視聴のたびにコア部分をサーバから受信して復号化する必要があり、これにより不正なコンテンツの利用を防止することが可能となる。また、コンテンツ全体ではなく、比較的データ量の少ないコア部分のみが暗号化されているので、サーバにおけるコア部分の暗号化やクライアントにおけるコア部分の復号化による認証処理の処理負荷も小さくすることができる。

## 【0048】

また、非コア部分のみがクライアント30内に保存されていても、コア部分が欠落した状態ではコンテンツ全体として価値がないようにコア部分を構成しておくことにより、例えば、クライアント30から一次要求がない状態で、サーバ20からクライアント30へあるコンテンツの非コア部分のみを送信しておき、希望する利用者からコア部分の補完要求があったときコア部分を送信することもできる。この方法は、有料コンテンツの非コア部分のみを無料でクライアントへ提供し、関心を持った利用者からの補完要求に対して有料でコア部分を送信するというコンテンツの提供サービスを可能とする。

## 【0049】

なお、図4(a)では、コア部は1つのまとまりとなっている例を示しているが、通信の速度や単位、データの単位等に応じてコア部を適宜分割してもよく、非コア部に対応させて、コア部a、コア部b、コア部cのように分割してもよい。

## 【0050】

## (コア部分の決定)

次に、コア部分の決定に関して説明する。本システムでは、コンテンツの一部であるコア部分をどのように決定するかが重要である。本実施例では、基本的にコア部は、例えばMPEG(Moving Picture Experts Group)ストリームの特定部分、例えばヘッダ部分やプログラムのメイン部分など、コンテンツの本質的な価値の中核であり、かつ、それ以外の非コア部分からは推測、構築不可能なものとする。また、コア部分は、上述のようにクライアントにおけるコンテンツの使用時に比較的短時間で認証が可能なデータサイズとする。

## 【0051】

より具体的な例では、例えばMPEGの動画コンテンツの場合、Iピクチャーをコア部分とすることにより、そこから次のIピクチャーまではコア部分なしでは画像を再構成できなくなる。また、映画やドラマなどのストーリーを有するコンテンツの場合、「重要シーン」や「最終回」など、ストーリーにおける重要部分をコア部分に設定することにより、その部分なしではストーリー全体の価値が

著しく低下するようにすることができる。また、そのようなコンテンツにおける時間情報に着目し、例えば映画の最後の30分間など、一般的にストーリー中の重要部分をなす部分をコア部分とすることができる。

#### 【0052】

また、映画やTV番組などのコンテンツにおいて、当該コンテンツに関する内容データや番組データなどが存在する場合には、それに基づいてコア部分を決定することができる。例えば映画の内容データやTV番組などの番組データ中にストーリー上重要な部分を示すクライマックス情報の如きが含まれている場合には、その情報が示す部分をコア部分とすることができる。さらに、コンテンツが例えば所定のプログラムなどの場合には、そのプログラムの実行において不可欠なメイン部分や定数などをコア部分とすることができる。

#### 【0053】

以上のようなコア部分をどのように定めるかは、基本的にはコンテンツ毎に予め人為的に決定することになるが、それが決定された後は、コア部分を抽出する処理自体は自動化される。例えば上述のように、Iピクチャーをコア部分とする、又は、映画の最後の30分をコア部分とする、ということが人為的に決定された後は、サーバ30が所定のプログラムを実行することにより、自動的にコンテンツデータ中からIピクチャーを抽出したり、映画コンテンツの最後の30分のコンテンツデータを抽出したりして、それをコア部分12とする。また、この他にも、例えば、映画などの動画コンテンツの場合には、画像の動きやコンテンツデータ中の各種ヘッダ情報などに基づいてシーンチェンジや重要シーンをコンテンツデータから自動検出し、コア部分に設定することができる。

#### 【0054】

具体的には、例えば図5に示すように、サーバ20内にコンテンツ分析部17を設ける。コンテンツ分析部17は、コンテンツデータの入力を受け取ると、上述のヘッダ情報や画像の動き情報などに基づいてコア部分を決定し、切り替え信号18を生成する。切り替え信号18はコア部分と非コア部分とを区別する信号であり、切り替え信号18に基づいてスイッチSWを制御し、コンテンツ分析部17から出力されるコンテンツデータをコア部分と非コア部分に区別して出力する

ことができる。

#### 【0055】

なお、以上の記載から理解されるように、本発明におけるコンテンツには、画像や音声情報のみならず、プログラムの如き情報も含まれる。

#### 【0056】

(コア部分の処理)

次に、コア部分に対する各種処理について説明する。なお、以下の例は、サーバ20から複数のクライアント30へ同一のコンテンツについてのコア部分を送信する場合のものである。

#### 【0057】

図6(a)はサーバ20から複数のクライアント30に対してコア部分12を送信する際の基本形を示す。サーバ20は各クライアント30へ同一のコア部分12を送信する。この態様では、各クライアント30は各々が暗号化されたコア部分12を復号化することにより、同一のコア部分12を取得する。こうすると、複数クライアントのユーザが共謀してコア部分を補完し合うことを防止できる。即ち、複数クライアントに対するコア部分が異なる場合、各ユーザがそれぞれのコア部分を復号化してそれらを持ち寄ることにより、コンテンツ全体を取得することができてしまうが、全てのクライアントへ送信するコア部分を同一とすることにより、そのような問題を防止することができる。

#### 【0058】

一方、図6(b)はサーバ20から複数のクライアント30に対して異なるコア部分12を送信する方法を示す。この場合、各クライアント30で復号化により得られるコア部分は互いに相違する。よって、例えばあるコア部分が不正に複製され、頒布されている場合には、コア部分を特定することによりその行為がどのユーザにより行われているかを追跡することができる。例えば図6(b)の例において、コア部分Bが不正に複製、頒布されている場合には、その行為はユーザYにより行われているとの推測が可能である。

#### 【0059】

これは、より具体的には、どのクライアント(ユーザ)に対してどのコア部分

を送信したかをサーバ20内の管理情報記憶部22内に記憶しておくことにより実現できる。また、他の方法としては、コア部分に各ユーザのIDやクライアントIDなどを含めて送信することによっても実現することができる。また、クライアントIDの代わりに、ユーザ毎に異なる電子透かしなどを含めることも可能である。

#### 【0060】

次に、コア部分を複数の部分により構成する手法について説明する。これまでの例では、基本的にコア部分は1つとしていた。これに対し、図7(a)に示すように、コア部分12を共通コア部分12aと個別コア部分12bとにより構成することができる。そして図7(b)に示すように、各クライアントへは共通コア部分と、相互に異なる個別コア部分との組み合わせを送信する。これにより、図6(a)の場合のように共通コア部分により複数クライアントが共謀してコンテンツを補完しあうことを防止できるとともに、図6(b)の場合のように不正に複製などされたコア部分の送信対象ユーザを特定することによりそのような不正行為の主体を特定することができる。

#### 【0061】

(サーバによる管理)

次に、サーバによるコア部分の管理について図8を参照して説明する。図6(b)の場合は、各クライアントに異なるコア部分を送信することにより、不正行為の主体を特定することができるというものであった。図8はその具体的な一例を示す。この例では、図8(a)に示すようにコンテンツ10は部分A～部分Dの4つの部分からなる。サーバ20は、ユーザXのクライアント30に対しては、部分A～Cを非コア部分11として、部分Dをコア部分12として送信する。また、サーバ20は、ユーザYのクライアント30に対しては部分A、B及びDを非コア11部分として、部分Cをコア部分12として送信する。同様に、サーバ20は、ユーザZのクライアント30に対して、部分A、C及びDを非コア部分11として、部分Bをコア部分12として送信する。同時に、サーバ20は、管理情報記憶部22内に、各ユーザX～Zに対するコア部分が部分A～Dのどれであることを記憶しておく。これにより、サーバ20は常にどのクライアント(ユ

ーザ) に対してどのコア部分が送信されているかを把握することができる。

#### 【0062】

次に、サーバによるコア部分の管理の別の手法について、図9を参照して説明する。図8の例ではどのクライアントに対してコンテンツのどの部分をコア部分として送信したかをサーバ20内に記憶している。図9の例では、既にクライアントへ送信済みである非コア部分を特定する情報をクライアントからの補完要求に含めることにより、サーバ20からクライアント30へ送信すべきコア部分を特定するものである。なお、図9においても送信するコンテンツは図8(a)に示す構成であるとする。

#### 【0063】

図9に示すように、クライアント30に既に非コア部分として部分A～Cが送信済みであるとする。このとき、クライアント30は既に保有している非コア部分A～Cから抽出あるいは計算した値、例えばhash値(ハッシュ(hash)関数により計算した値)等の、非コア部分を特定するための特定情報を認証情報として補完要求に含めてサーバへ送信する。サーバ20はこの補完要求を受け取り、認証処理としてhash値を参照することにより、その補完要求の送り主であるクライアントの認証を行い、そのクライアントが非コア部分A～Cを保有していることを知る。そして、不足している部分Dをコア部分に決定し、所定の暗号化を施してクライアントへ送信する。これにより、サーバ20はクライアント30から受信する補完要求中のhash値などに基づいて補完要求に関する認証を行い、送信すべきコア部分を決定することができる。

#### 【0064】

また、クライアント30は、上記hash値などの非コア部分の特定情報を暗号化してサーバ20へ送信することができ、その際の暗号化の鍵情報は、クライアント30が当該特定情報を暗号化する時刻情報とすることができる。

#### 【0065】

また、上記の例では、hash値などの非コア部分の特定情報を利用して認証処理を行っているが、その代わりに、非コア部分自体又はその一部などを認証情報として利用してもよい。

**【0066】**

なお、上記の説明は、クライアントからの補完要求についての例であるが、補完要求ではなく、単にサーバ20からクライアント30へ送信された非コア部分の受領確認に同様の手法を適用することもできる。即ち、クライアント30が補間要求を行う場合ではなく、サーバ20から非コア部分11を受信した際に、それらを確かに受信したことをサーバ20へ通知するために上記の手法を利用することができる。例えばあるクライアント30が非コア部分A～Cを受信した際には、直ちに又は所定のタイミングで、それら非コア部分A～Cから抽出あるいは計算した値（上記のhash値など）を、受領確認情報としてサーバ20へ送信するようにする。サーバ20は、そのhash値などを受信し、参照すれば、クライアント30から要求された非コア部分A～Cが確かにそのクライアント30へ配信されたことを確認することができる。

**【0067】**

また、サーバ20は、クライアント30へコア部分を送信する度に、その送信履歴をログ情報として記憶し、さらにはそのログ情報をクライアント30へも送信することができる。その場合、クライアント30は上記のhash値の代わりに、ログ情報（例えばある日時にサーバ20から非コア部分A～Cを受信したことを示す）を認証情報として補完要求に含めてサーバ20へ送信する。サーバ20はこのログ情報を受信することにより、その発信元であるクライアントの認証を行い、そのクライアントに対してコア部分として部分Dを送信することを決定することができる。

**【0068】**

また、そのようなログ情報は、クライアント30において起こりうる不正行為などの検出に利用することもできる。例えば、サーバ20が定期的にクライアント30にアクセスし、過去に送信したコンテンツに関するログ情報を取得してサーバ20内に保存してあるログ情報と照合する。両者が一致しない場合は、サーバ20は、クライアント30において何らかの改変などが行われていると判断することができる。また、クライアント30内のログ情報を取得し照合するタイミングは、定期的に設定する他に、例えばクライアント30からサーバ20へ補完

要求がなされたときとすることもできる。

【図面の簡単な説明】

【図 1】

本発明の実施形態に係るコンテンツの構成、及び、基本的なコンテンツ提供形態を模式的に示す。

【図 2】

実施例に係るコンテンツ提供システムの構成例を示すブロック図である。

【図 3】

実施例に係るコンテンツ提供システムの他の構成例を示すブロック図である。

【図 4】

実施例に係るコンテンツ提供システムの基本動作を示す図である。

【図 5】

コンテンツのコア部分と非コア部分の自動生成のための構成例を示す。

【図 6】

コア部分の送信方法を例示する図である。

【図 7】

コア部分の送信方法を例示する他の図である。

【図 8】

コンテンツの送信方法を例示する図である。

【図 9】

サーバによるコンテンツ提供の管理形態を示す図である。

【符号の説明】

10 コンテンツ

11 非コア部

12 コア部

1、20 サーバ

2 30 クライアント

21 コンテンツデータ記憶部

22 管理情報記憶部

2 3、3 2 コントロール部

2 4、2 5、3 1、3 5 通信部

3 3 一時記憶部

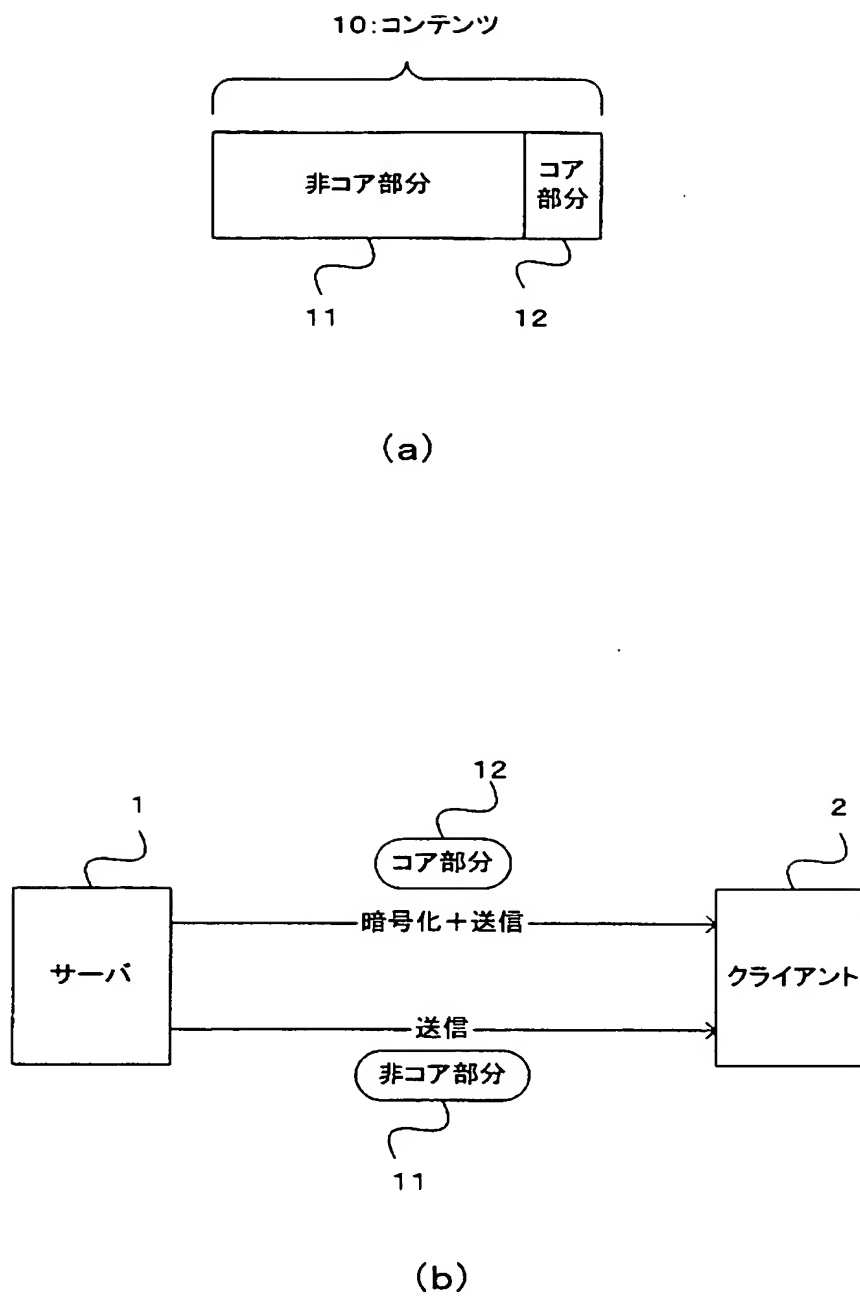
3 4 提示部

4 0、4 1 通信路

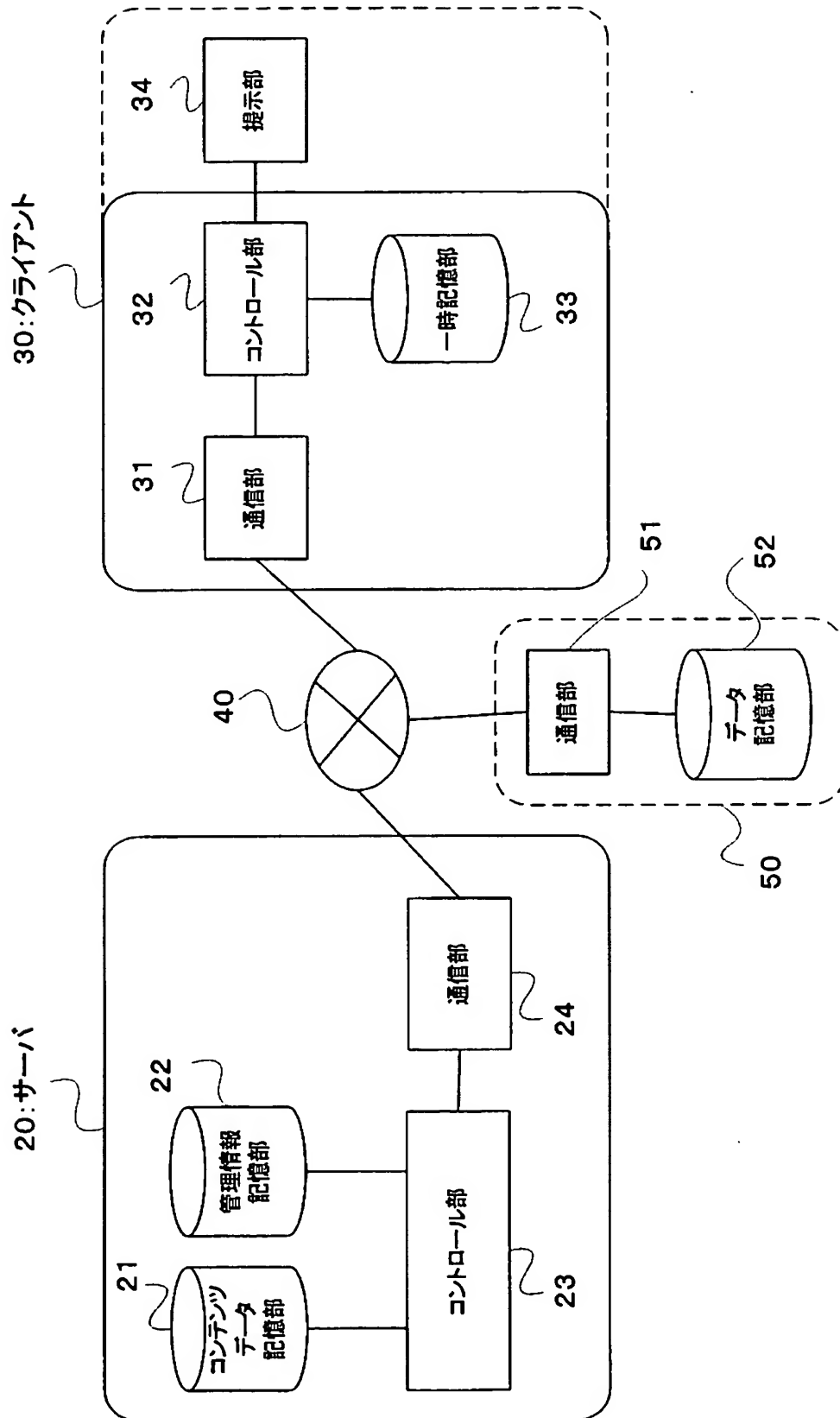
【書類名】

図面

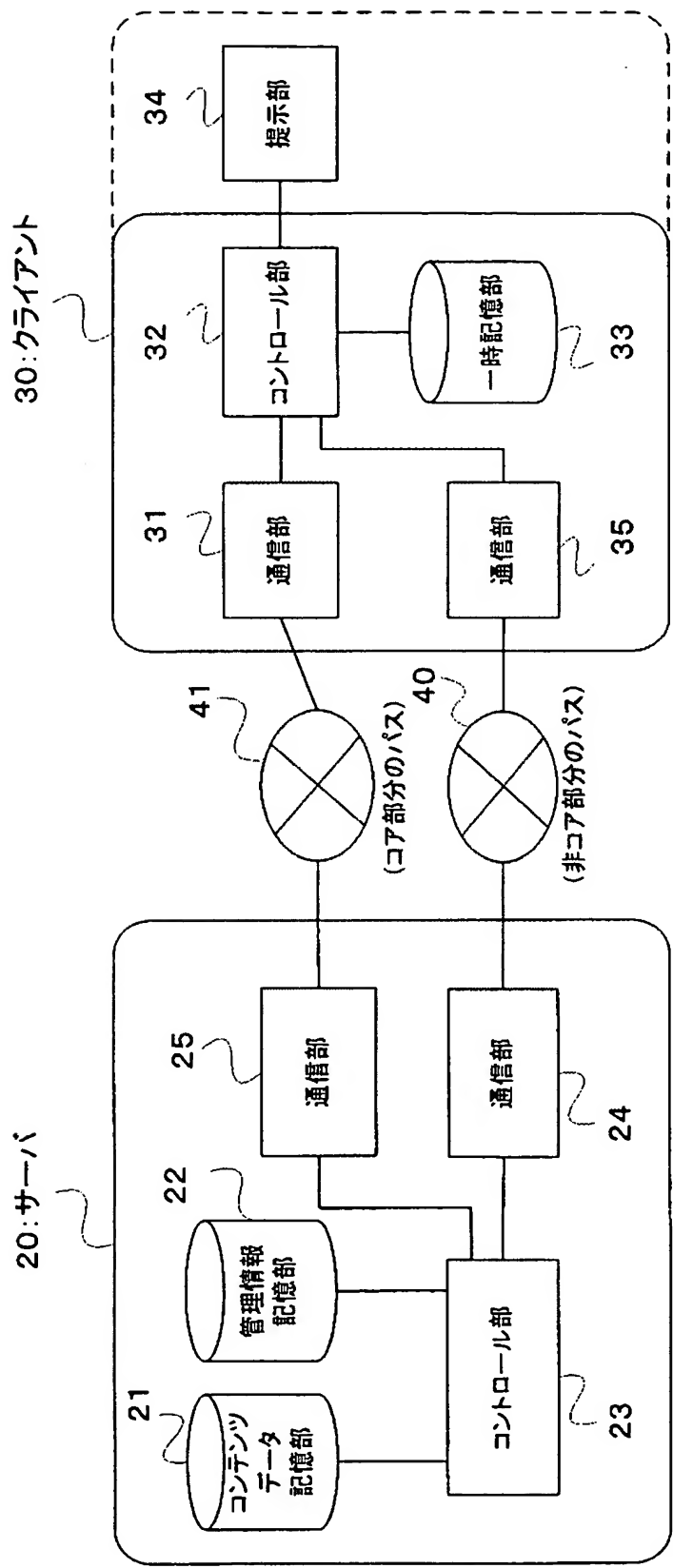
【図 1】



【図 2】



【図 3】

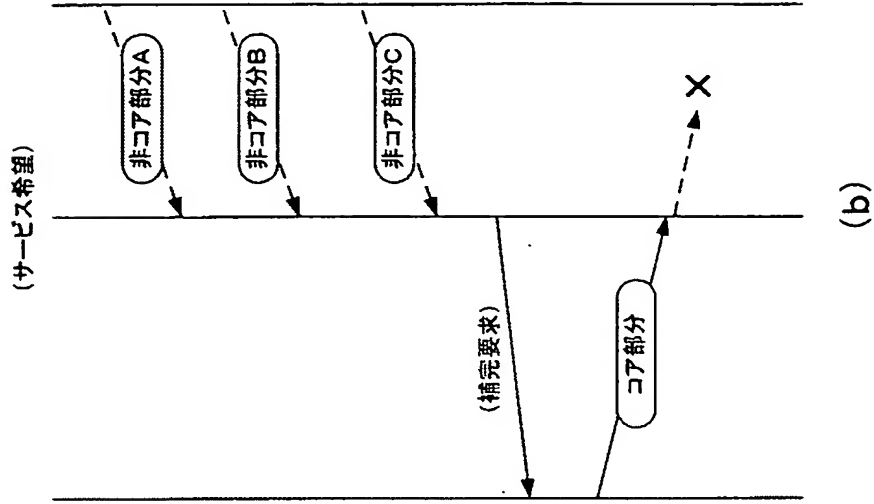


【図4】

2回目以降の視聴

<クライアント> <クライアント記憶部>

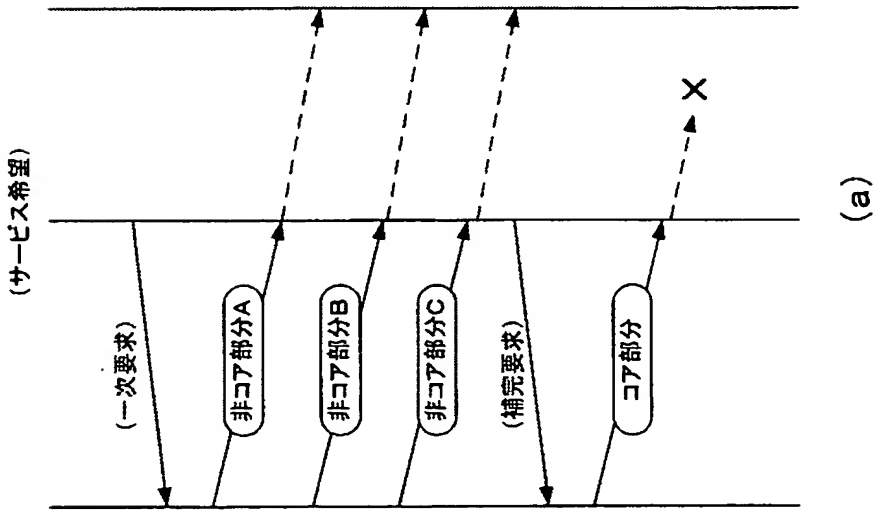
<サーバ>



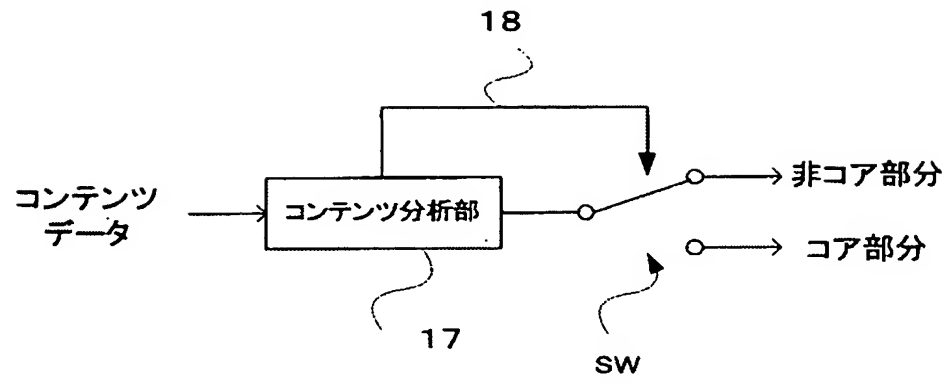
初回の視聴

<クライアント> <クライアント記憶部>

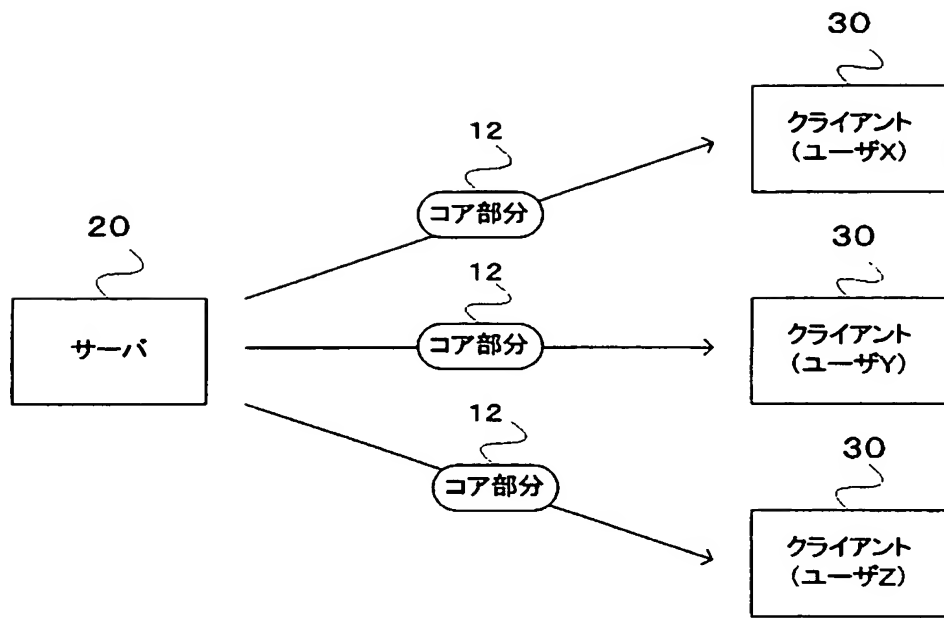
<サーバ>



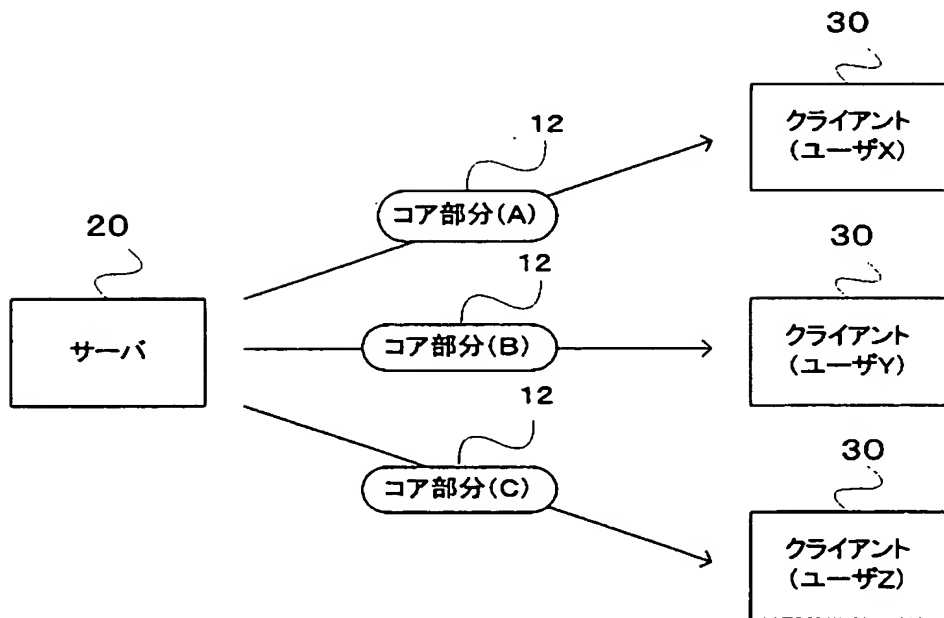
【図 5】



【図 6】

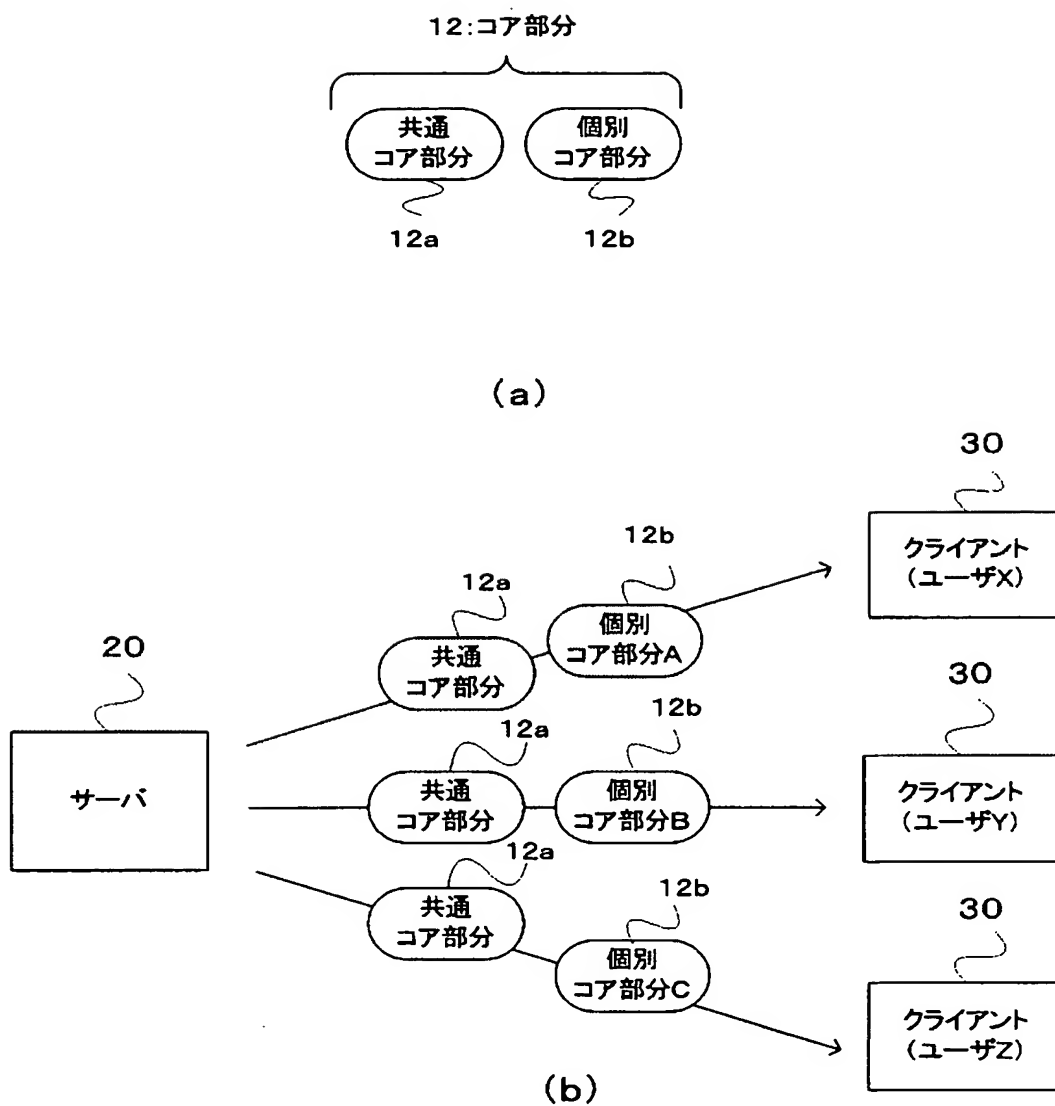


(a)

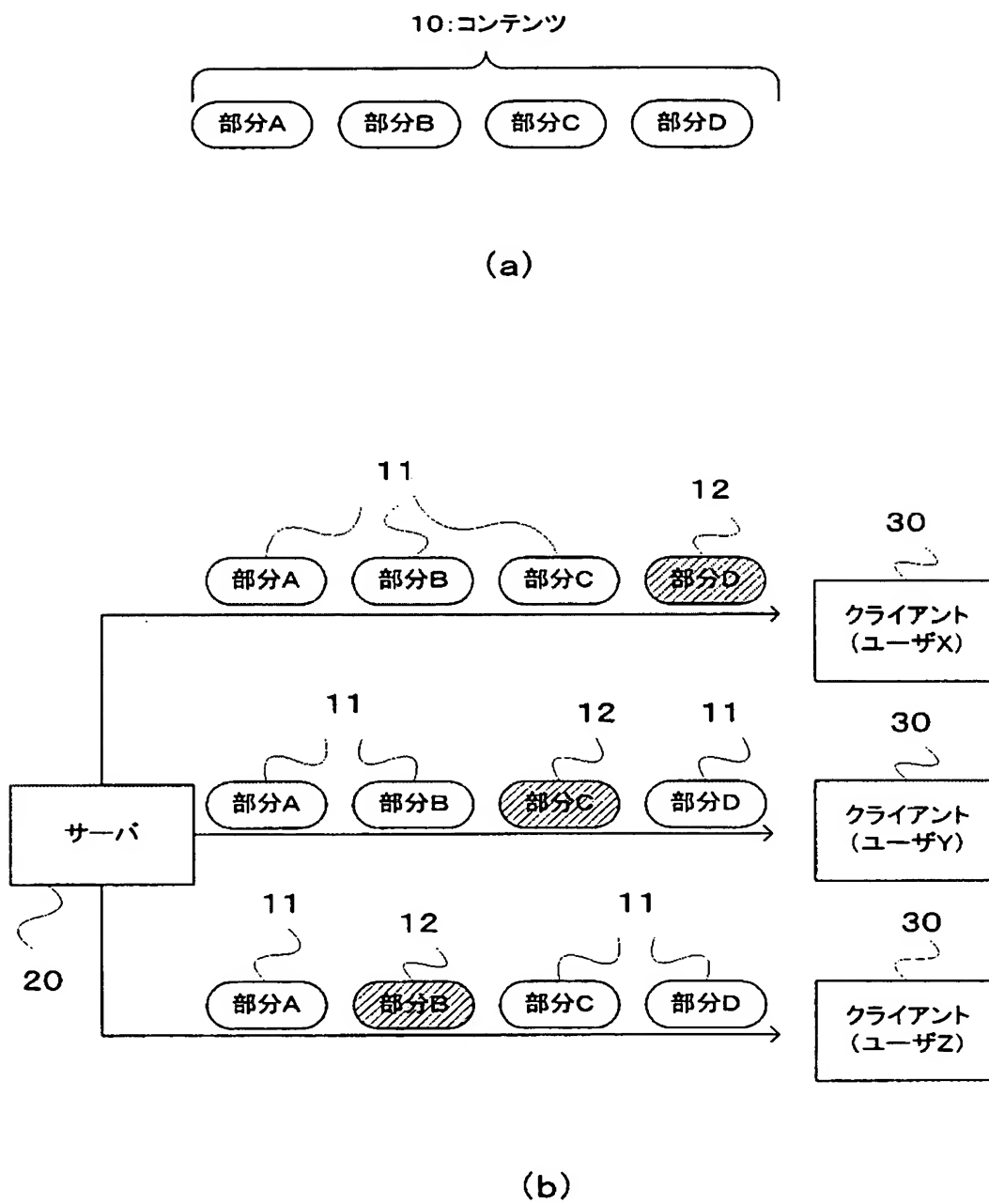


(b)

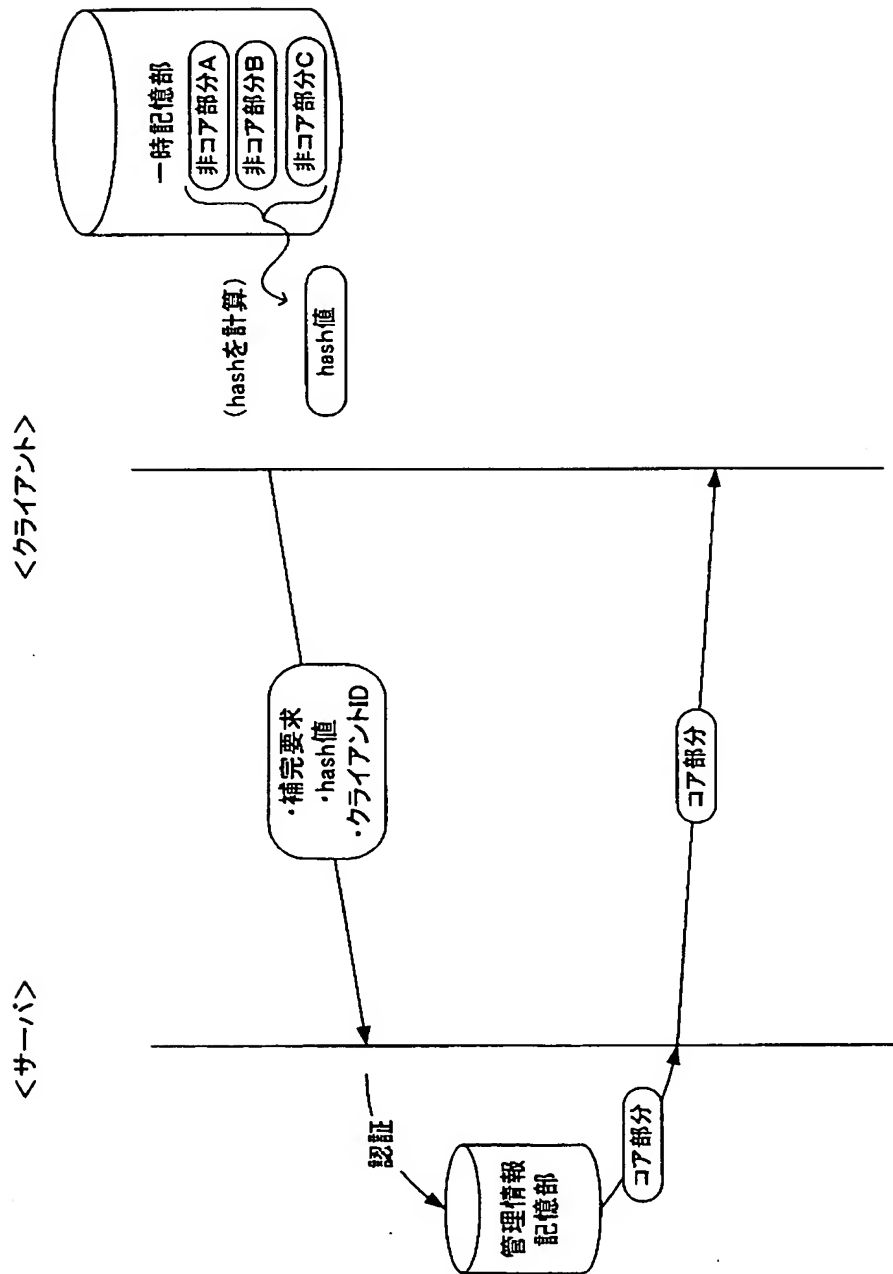
【図 7】



【図 8】



【図 9】



【書類名】 要約書

【要約】

【課題】 コンテンツの一部を分割して提供する方法において、分割や提供方法を工夫することにより、コンテンツの不正な複製や使用などを効果的に防止する。

【解決手段】 利用者へ提供すべきコンテンツをコア部分と非コア部分とに分け、コア部分に必要な暗号化処理などを施してクライアントへ提供する。コンテンツの重要部分をコア部分とし、これを暗号化して送信するので、コア部分のみの暗号化処理によりコンテンツ全体を実質的に保護することが可能となる。

【選択図】 図 2

特願 2 0 0 3 - 0 8 2 8 1 0

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 0 1 6 ]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都目黒区目黒 1 丁目 4 番 1 号

氏 名

パイオニア株式会社